

UNITED STATES DISTRICT COURT
DISTRICT OF NORTH DAKOTA

SpoofCard, LLC and Amanda Pietrocola,

Plaintiffs,

vs.

The Hon. Doug Burgum, Governor of the
State of North Dakota, in his Official
Capacity,
and

The Hon. Wayne Stenehjem, Attorney
General of the State of North Dakota, in his
Official Capacity,

Defendants.

Case No.

COMPLAINT

I. NATURE OF THE ACTION

1. On April 11, 2019, Governor Doug Burgum signed into law HB 1161, the North Dakota “Caller ID Anti-Spoofing Act” (the “Act” or “Anti-Spoofing Act”). The Act went into effect on August 1, 2019. A copy of the Act is attached as Exhibit A.

2. The Anti-Spoofing Act adds a new section to the North Dakota Century Code, at section 51-28-08.1, that makes it illegal to “knowingly cause any telephone caller identification system to: a. Transmit misleading or inaccurate caller identification information with the intent to defraud or cause harm; or b. Use or display a telephone number the caller does not own or has not received consent to use from the owner of the telephone number.” The Anti-Spoofing Act also provides that “‘Defraud’ means taking anything of value, *including . . . time*, without consent from the recipient of a call.”

3. Under the Act, any person who violates either of those prohibitions “is guilty of a Class A misdemeanor . . .,” which is punishable by fines or imprisonment under North Dakota law. In addition, such person is subject to potentially substantial civil liability in an action brought by the recipient of a spoofed call:

3. Any person who receives a call in violation of subsection 1 may bring a civil action in a court of this state in the county in which the call recipient resides to enjoin such action, or for damages, or both. If the plaintiff prevails, the court must award the plaintiff the plaintiff's actual damages or damages in an amount not less than five thousand dollars and not more than ten thousand dollars per violation, whichever is greater. Each call is a separate violation under this chapter. The court shall award the plaintiff's costs, expenses, and reasonable attorney's fees. The relief provided in this section is in addition to all remedies available to the attorney general under this chapter in any investigation or action brought by the attorney general against the caller in the plaintiff's private action. This section may not be interpreted to limit any other claims the person may have against the caller or any other claims the attorney general may bring under this chapter, chapter 51-15, or any other state or federal laws.

4. Plaintiffs bring this action under 28 U.S.C. §§ 2201 and 2202 seeking a declaration that the Anti-Spoofing Act is in conflict with, and therefore preempted by, the federal Truth in Caller ID Act of 2010, Public Law 111-331, 47 U.S.C. § 227(e), and that the Act is unconstitutional, both on its face and as applied to Plaintiffs. Plaintiffs seek a permanent injunction preventing enforcement of the Anti-Spoofing Act.

II. PARTIES, JURISDICTION, AND VENUE

5. Plaintiff SpoofCard LLC (“SpoofCard”) is a limited liability company incorporated outside of North Dakota with its headquarters in New Jersey. It offers the SpoofCard service, which operates like a regular long distance calling card service, but also provides each customer the capability to alter (or “spoof”) the caller ID that is displayed on a

called party's telephone. The SpoofCard service is the most widely used service of its type offered to consumers in the United States, with approximately 500,000 active users. SpoofCard provides and intends to continue to provide its customers the ability to make voice telephone calls to and from North Dakota using caller ID spoofing. On an average day, dozens or hundreds of SpoofCard customers may make interstate telephone calls to or from North Dakota using caller ID spoofing.

6. Plaintiff Amanda Pietrocola is a resident of New Jersey and is the chief executive officer of SpoofCard. She is also a user of the SpoofCard service who has made interstate calls to, and intends in the future to make interstate calls to or from, North Dakota using caller ID spoofing.

7. Defendant Doug Burgum is the Governor of the State of North Dakota and is being sued in his official capacity.

8. Defendant Wayne Stenehjem is the Attorney General of the State of North Dakota and is being sued in his official capacity.

9. This Court has subject matter jurisdiction over the action and personal jurisdiction over the Defendants, and venue is proper in this district.

10. This case arises under the United States Constitution and the laws of the United States and presents a federal question within this Court's jurisdiction under Article III of the federal Constitution and pursuant to 28 U.S.C. § 1331.

11. Personal jurisdiction exists over the defendants under Federal Rule of Civil Procedure 4(k)(1)(A) and North Dakota Rule of Civil Procedure 4(b)(1).

12. Venue is proper in this district under 28 U.S.C. § 1391.

13. Injunctive relief is available as a remedy under Fed. R. Civ. Proc. 65.

III. FACTS APPLICABLE TO ALL CLAIMS

A. Nature of Caller ID Spoofing and the SpoofCard Service

14. Caller ID is a communications service that transmits to a called party the number from which a telephone call is apparently being made. The information is transmitted to the called party's telephone equipment before the call is answered. The caller ID information is usually displayed on the called party's telephone or on a separate but connected device. Depending on the sophistication of the called party's equipment, it may also provide to the called party a name associated with the caller ID. For example, a caller ID of 202-456-1414 should be associated with the name "White House" in a caller ID display.

15. A regular phone call over the public switched telephone network (the "voice network" or "PSTN") is set up through the use of the Signaling System 7 ("SS7") out-of-band signaling system used by the landline (or "fixed line") telephone company switches to connect, maintain and bill for the call. The caller ID can be derived from the Automatic Number Identification ("ANI") or the Called Party Number ("CPN"), two of the SS7 data fields.

16. Many types of telephone equipment and software programs permit the caller to manipulate the caller ID by changing the CPN or, where there is no CPN, inserting data that SS7 reads as the CPN. For example, private branch exchanges ("PBXes") and other telephony hardware products made by dozens of manufacturers, including Nortel, Alcatel, Huawei, Lucent and Pingtel, all provide this capability. These products have been used for decades by millions of businesses. In addition, since 2000 several free open source software programs, including Asterisk, FreeSwitch and SIPexchange, have been developed that provide equivalent PBX

capability, including caller ID spoofing. These programs are free and can be run on any server or high-end personal or laptop computer.

17. Today a telephone call to someone on the PSTN need not be initiated from another telephone on the PSTN. In fact, a growing number of calls are made from other voice networks, such as mobile networks, or from the internet using a device based on Internet Protocol (“IP”) technology, such as a computer, a smartphone, or an ATA (analog telephony adapter). On such an IP call, there is no PSTN number (and therefore no caller ID) associated with the caller or the device. Thus, many service providers input a default number that by definition “misleads” the called party about the identity of the caller. For example, unless a caller selects otherwise, Skype automatically inserts a default caller ID of 000123456 for all Skype-Out calls that originate in the U.S. (Skype-Out calls are calls from a device running Skype software to a number on the PSTN.)

18. Many service providers offering IP to PSTN calling do not insert a uniform caller ID for all calls, as Skype does, but offer customers the capability of customizing their communication by allowing a customer to input a number and having that number transmitted by the IP network and read by the PSTN as a caller ID.

19. The process of using the SpoofCard service is essentially the same whether the customer is using a landline, a mobile phone or a computer to make a call. In each case, the customer will dial a local access number (also known as an inbound DID) to initiate the call. This is the same for all calls, whether they are set up on the web or within the mobile application.

20. The call is routed through the DID to a cloud-based communications provider from whom SpoofCard purchases inbound DID numbers and transport services. This inbound carrier converts the call from TDM format to internet protocol (IP) format if necessary (computer

and some mobile phone calls are already in IP format), then transmits the call through a Session Initiation Protocol (“SIP”) gateway and over its network to a cloud computing service (such as Google Cloud) where SpoofCard is running FreeSwitch, the soft switch program that SpoofCard uses.

21. When the call reaches the SpoofCard server, FreeSwitch runs a validation query on the phone number that the user wishes to display on their caller ID in order to ensure that it is a valid phone number and that it is not on SpoofCard’s “do not spoof” list. If the number is validated, the requested change is made so that when the call is completed, it will appear to the receiving party’s carrier that the call originated from the substituted caller ID. At the same time, SpoofCard checks the called number to ensure it does not appear on the SpoofCard Do Not Call list. For example, 911 centers and certain numbers for law enforcement agencies and financial services companies are on the list, so customers cannot make calls with spoofed caller ID to them.

22. The outbound call (still in IP format) is routed from the cloud computing servers over a different cloud-based communications provider network to the called party’s network provider. Depending on their interconnection arrangements, either the transit provider or the called party’s network converts the call to TDM format and thus bridges the calling phone with the receiving phone via the PTSN.

IV. THE FEDERAL LAW GOVERNING CALLER ID SPOOFING ON INTERSTATE CALLS

23. Until the enactment of the federal Truth in Caller ID Act of 2010, Public Law 111-331, 47 U.S.C. § 227(e), spoofing the caller ID on any interstate call was legal. In enacting the Truth in Caller ID Act, Congress specifically decided that caller ID spoofing

should be legal on interstate calls unless the calls are made with intent to “defraud, cause harm, or wrongfully obtain anything of value.”

24. The legislative history of the Truth in Caller ID Act demonstrates beyond doubt that Congress intended that spoofed calls that were not made with the intent to “defraud, cause harm, or wrongfully obtain anything of value” were to remain legal. *TelTech Systems, Inc. v. Bryant*, 702 F.3d 232, 237 (5th Cir. 2012).

V. THE ANTI-SPOOFING ACT

25. Section 1 of the Anti-Spoofing Act creates a new section in chapter 51-28 of the North Dakota Century Code that makes it illegal for a person to “knowingly cause any telephone caller identification system to: a. Transmit misleading or inaccurate caller identification information with the intent to defraud or cause harm; or b. Use or display a telephone number the caller does not own or has not received consent to use from the owner of the telephone number.” See N.D.C.C. § 51-28-08.1. Section 5(c) of the Anti-Spoofing Act also provides that “‘Defraud’ means taking anything of value, *including . . . time*, without consent from the recipient of a call.”

26. The Act imposes criminal liability on any person who violates either of those prohibitions. Any such person “is guilty of a Class A misdemeanor . . .,” which is punishable by imprisonment or fine under North Dakota law.

27. In addition, such person is subject to civil suit:

3. Any person who receives a call in violation of subsection 1 may bring a civil action in a court of this state in the county in which the call recipient resides to enjoin such action, or for damages, or both. If the plaintiff prevails, the court must award the plaintiff the plaintiff’s actual damages or damages in an amount not less than five thousand dollars and not more than ten thousand dollars per violation, whichever is greater. Each call is

a separate violation under this chapter. The court shall award the plaintiff's costs, expenses, and reasonable attorney's fees. The relief provided in this section is in addition to all remedies available to the attorney general under this chapter in any investigation or action brought by the attorney general against the caller in the plaintiff's private action. This section may not be interpreted to limit any other claims the person may have against the caller or any other claims the attorney general may bring under this chapter, chapter 51 - 15, or any other state or federal laws.

* * *

28. Section 2 of the Act provides a number of exceptions to the broad potential liability. Two of those are relevant to this case. Section 2(d) provides a specific exemption from potential liability for a "telecommunications, broadband, or voice over internet protocol service provider acting solely as an intermediary for the transmission of telephone service between the caller and the recipient." Section 2(f) exempts a "caller who, based on the telephone number called, reasonably believes the recipient of the call is not physically within the state."

29. The plain language of the Anti-Spoofing Act prohibits any use of caller ID spoofing where either the calling or called party is physically in North Dakota, unless one of the exceptions in Section 2 applies. Because there is no geographic limitation, this provision by definition also covers interstate calls, where one party to the call is located outside of North Dakota.

VI. THE EFFECT OF THE ANTI-SPOOFING ACT

30. Any communications service provider such as Plaintiff SpoofCard faces potential criminal liability under the Anti-Spoofing Act unless it qualifies under Section 2(d) as a "telecommunications, broadband, or voice over internet protocol service provider acting

solely as an intermediary for the transmission of telephone service between the caller and the recipient.”

31. SpoofCard does not qualify for this exception because it is not a telecommunications, broadband, or voice over internet protocol service provider. Therefore, SpoofCard has potential liability under the Anti-Spoofing Act for the actions of its customers.

32. It is impossible for any user of caller ID spoofing, or for SpoofCard or any other provider of voice services that offers caller ID spoofing, to ensure that it is complying with the Act no matter how hard it tries. In order to be sure it is complying, a caller or a service provider must know both where the call is originating from and where the called party is located. Back when all telephones were landline phones connected to wall jacks, determining where calls began and ended was easy. This is no longer true.

33. Given the present state of communications technology, neither a customer using caller ID spoofing nor any communications service provider, such as Plaintiff SpoofCard, can be sure anymore where a party receiving a spoofed call is actually located.

34. In addition, many communications service providers, particularly VoIP providers, mobile carriers and calling card companies, also may not know where their own customers are located when they make or originate a call.

35. The reason that neither a caller ID user nor a communications service provider can be sure any more where a called party is actually located (or, in some cases, even where a call originates) is that four technological and regulatory developments in recent years have de-coupled the century-old link between the telephone number and the geographic location of the telephone user. These are (1) the tremendous growth of mobile phone usage (and its

substitution for fixed or landline PSTN phone service), (2) the introduction of IP-base services, including VoIP, that interconnect with the old PSTN, (3) the imposition of number portability by the Federal Communications Commission (“FCC”), and (4) the growth of call forwarding service on landline telephones.

36. The tremendous growth in mobile phone usage is well documented. As the FCC and the courts recognize, many people, for business or personal reasons, have a mobile number that is associated with an area code other than the one where they live or work. Moreover, even many people who live in the state associated with their mobile phone area code are making a substantial percentage of their calls from outside that state.

37. Similarly, there is no way to tell where many VoIP users are when they place a call or whether the call being placed is an interstate or intrastate call. A user of nomadic or mobile VoIP service can initiate or receive a call from anywhere in the world that he or she can find a broadband connection. Thus, there is no longer any automatic connection between the area code of a calling or called party’s number and the party’s location.

38. The effect of the growth of mobile and VoIP services has been exacerbated by the FCC’s implementation of number portability, which gives a customer the right and the ability to take (or “port”) his or her existing number when moving from one carrier to another *or one state to another*. Such porting is becoming more common, and many people are giving up their fixed landline service entirely and porting their fixed number to a VoIP or mobile carrier. Thus, every day a smaller percentage of total telephone calls are to or from fixed landline phones, the only phones whose location can ordinarily be expected to be within the geographic confines of the associated area code.

39. But even landlines are no longer tied to a geographic location, because there has been tremendous growth in call forwarding services. Such services are offered by landline telephone companies for free as part of their business packages and for free or as part of a bundled “unified communications” or “follow me” package by many new competitors (e.g., 8 x8 (see <https://www.8x8.com/unified-communications/ucaas>) or Google Voice (see <http://www.google.com/voice>)). With the confluence of number portability and call forwarding, even a substantial percentage of calls that appear to be to landline phones in a specific area code are in fact terminated at phones outside the state to which that area code is assigned.

40. Given all these developments, it is not possible for a caller or service provider to know for certain where a called party is located. It may not even be possible in many cases for the service provider to know where the calling party - its own customer - is located. For example, Plaintiff SpoofCard has no way of knowing whether any of its customers are placing a call from a computer or from a mobile phone are in North Dakota.

41. It is possible for software technology used in providing telecom services to block calls to or from specific area codes, including those in which the numbers generally correspond to geographic locations in North Dakota. However, any attempt to block such calls would be both over-inclusive (because it would include calls made by or to mobile users and nomadic VoIP subscribers with North Dakota area code numbers but who are actually located outside of North Dakota) and under-inclusive (because it would not include calls made by or to mobile users or nomadic VoIP subscribers with non-North Dakota area code numbers but who are actually located in North Dakota when the calls are made). Therefore, blocking calls to North Dakota area codes cannot ensure that no calls to or from

North Dakota use caller ID spoofing services. Moreover, such blocking would prevent users in other states from using services which are legal in those states.

42. On its face, the Anti-Spoofing Act also prohibits various forms of constitutionally protected speech, including anonymous speech, pseudonymous speech, and the use of false identification to avoid social ostracism, to prevent discrimination and harassment, and to protect privacy.

COUNT I
CONFLICT WITH AND PREEMPTION BY GOVERNING FEDERAL LAW

43. Plaintiffs restate and incorporate by reference each and every allegation in Paragraphs 1 through 42 as if fully set forth herein.

44. The Anti-Spoofing Act violates the Supremacy Clause (Article VI, Clause 2) of the United States Constitution, which provides that “[t]his Constitution, and the Laws of the United States which shall be made in Pursuance thereof; . . . shall be the supreme Law of the land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding.”

45. The Anti-Spoofing Act conflicts in substantial part with, and therefore is preempted by, 47 U.S.C. § 227(e), part of the federal Truth in Caller ID Act of 2010. The conflict lies in the fact that Congress specifically decided that caller ID spoofing should be legal on interstate calls unless the calls are made with intent to “defraud, cause harm, or wrongfully obtain anything of value,” while the Act makes a wide array of such calls illegal in interstate commerce involving North Dakota. The conflict prevents the achievement of the Congressional purpose underlying the enactment of the Truth in Caller ID Act of 2010.

COUNT II
VIOLATION OF THE INTERSTATE COMMERCE CLAUSE

46. Plaintiffs restate and incorporate by reference each and every allegation in Paragraphs 1 through 45 as if fully set forth here.

47. The Anti-Spoofing Act effectively prohibits the spoofing of caller ID on interstate telephone calls.

48. The Anti-Spoofing Act is unconstitutional because it violates the Interstate Commerce Clause (Article I, Section 8, Clauses 1 and 3) of the United States Constitution, which provides that “[t]he Congress shall have power . . . [t]o regulate commerce with foreign nations, and among the several states, and with the Indian tribes; . . .”

49. The Constitution and laws of the United States preempt the ability of the State of North Dakota to regulate the spoofing of caller ID on interstate telephone calls.

COUNT III
VIOLATION OF THE DORMANT COMMERCE CLAUSE

50. Plaintiffs restate and incorporate by reference each and every allegation in Paragraphs 1 through 49 as if fully set forth here.

51. The Anti-Spoofing Act violates the dormant Commerce Clause of the United States Constitution on its face because it will inevitably have an impermissible effect on interstate commerce conducted wholly outside the State of North Dakota.

COUNT IV
VIOLATION OF THE FIRST AND FIFTH AMENDMENT
RIGHT TO FREE SPEECH – OVERBREADTH AND VAGUENESS

52. Plaintiffs restate and incorporate by reference each and every allegation in Paragraphs 1 through 51 as if fully set forth here.

53. The First Amendment to the United States Constitution provides that “Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.” The Fifth Amendment provides that “[n]o person shall . . . be deprived of life, liberty, or property, without due process of law . . .”

54. The Anti-Spoofing Act violates the First and Fifth Amendments because it is substantially overbroad.

55. The Anti-Spoofing Act violates the First and Fifth Amendments because it is not the least restrictive means of accomplishing any compelling governmental purpose.

COUNT V
VIOLATION OF THE FIRST, FIFTH AND FOURTEENTH AMENDMENT RIGHT
TO COMMUNICATE

56. Plaintiffs restate and incorporate by reference each and every allegation in Paragraphs 1 through 55 as if fully set forth here.

57. Section 1 of the Fourteenth Amendment prohibits a state from trampling any of the First or Fifth Amendment freedoms. It provides in relevant part that “[n]o State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.”

58. The Anti-Spoofing Act is unconstitutional because it violates the First, Fifth and Fourteenth Amendments by denying citizens their right to communicate anonymously and pseudonymously.

COUNT VI
DECLARATORY JUDGMENT

59. Plaintiffs restate and incorporate by reference each and every allegation in Paragraphs 1 through 58 as if fully set forth here.

60. There is a real and actual controversy between Plaintiffs and Defendants regarding whether the Anti-Spoofing Act is preempted by federal law or is unconstitutional.

61. Plaintiffs seek a Declaratory Judgment pursuant to 28 U.S.C § 2201 and Fed. R. Civ. Proc. 57 for the purpose of determining and adjudicating questions of actual controversy between the parties.

62. Plaintiffs contend that the Anti-Spoofing Act

- a. Conflicts with and is therefore preempted by federal law;
- b. Is unconstitutional because it violates the Interstate Commerce Clause of the United States Constitution; and
- c. Is unconstitutional because it violates the First, Fifth and Fourteenth Amendments to the United States Constitution.

63. Plaintiffs are informed, believe and allege that Defendants contend the contrary of each of (a), (b) and (c).

64. Wherefore the Plaintiffs request that the Court determine and adjudge that each of the propositions in Paragraph 62 is correct, and that the Anti-Spoofing Act is both preempted by federal law and unconstitutional, and for each reason is therefore unenforceable.

COUNT VII
VIOLATION OF THE CIVIL RIGHTS ACT (42 U.S.C. § 1983)

65. Plaintiffs incorporate by reference each and every allegation in Paragraphs 1 through 64 as if fully set forth here and further allege as follows:

66. Defendants Burgum and Stenehjem are individuals who, under color of statute, ordinance, regulation, custom, or usage, of the State of North Dakota, are subjecting, or causing to be subjected, said Plaintiffs to the deprivation of rights, privileges, or immunities secured by the Constitution and laws of the United States—specifically, the Supremacy and Commerce Clauses of the United States Constitution.

67. Defendants' conduct violates 42 U.S.C. § 1983.

68. Without relief from this Court, Defendants, acting under color of statute, ordinance, regulation, custom, or usage of the State of North Dakota, will continue to subject, or cause to be subjected, the individual Plaintiff to the deprivation of rights, privileges, or immunities secured by the Constitution and laws of the United States.


PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for themselves and all others similarly situated that the Court enter an order:

1. Assuming jurisdiction of this action;
2. Declaring that the Anti-Spoofing Act is preempted by federal law and violates the Constitution and laws of the United States;
3. Enjoining Defendants, their agents, servants, employees, successors and assigns, and all others in concert or in privity with them, from bringing or threatening to bring any criminal prosecution or civil enforcement action, or from otherwise attempting to enforce, the Anti-Spoofing Act;
4. Awarding damages to Plaintiffs in an amount equal to damages proven at trial;
5. Awarding the Plaintiffs their reasonable attorney's fees and costs pursuant to 42 U.S.C. § 1988; and
6. Granting Plaintiffs such further relief as the Court may deem just and equitable.

Dated this 16 day of December, 2019

VOGEL LAW FIRM


BY: Seth A. Thompson (#07662)
US Bank Building
200 North 3rd Street, Suite 201
PO Box 2097
Bismarck, ND 58502-2097
Telephone: 701.258.7899

Email: sathompson@vogellaw.com
ATTORNEYS FOR PLAINTIFFS

Mark C. Del Biancoⁱ
Law Office of Mark C. Del Bianco
3929 Washington St.
Kensington, MD
D.C. Bar No. 3424246

ⁱ *Pro hac vice* motion to be submitted.